CHAPTER 4

THE CHALLENGE UNDER EXAMINATION

INTRODUCTION

Colonel Scott Forster

Director, Operations and Gaming Division
Center for Strategic Leadership

We have looked at strategic guidance and intent, and we have looked at the effect of those strategies and that guidance upon State and local government and within the private sector. We have looked at the road to a public-private partnership for CIP. Some are focused on the road; others, on the speed bumps. In this chapter we approach the issue from the standpoint of examining the challenges that await us as we continue our efforts to protect the Nation's critical infrastructure—modeling the threat and our ability to meet it, and devising means of measuring both our vulnerability and our preparedness.

Toward this end, Mr. Jon MacLaren of the Protective Services Division of the Information Assurance and Infrastructure Protection Division of DHS will offer his perspective on "Critical Infrastructure Protection: Mapping Threats against Vulnerabilities. Following Mr. MacLaren, Dr. Alok Chaturvedi will address "Simulating Attacks against Critical Infrastructure," based on his work as Director of the Homeland Security Institute at Purdue. Finally, Mr. Dan Mathis, the Deputy Program Manager and Director of Operations for the Defense Program Office for Mission Assurance, will address "Assessing Vulnerabilities to Critical Infrastructure."


Prudens
Futuri

Critical Infrastructure Protection: Mapping Threats Against Vulnerabilities

Jon MacLaren

Protective Services Division,
Information Assurance and Infrastructure Protection,
Department of Homeland Security

The Homeland Security Act and the DHS Strategic Plan clearly define the key activities that America must execute to protect critical infrastructure. These documents lay out the key objectives and tasks for infrastructure protection. We must protect the public from terrorism and other illegal activities, reduce infrastructure vulnerability to acts of terrorism, strengthen nationwide preparedness and mitigation, and ensure continuity of government operations and essential functions. In accomplishing these, we must begin by identifying critical infrastructure, prioritizing our efforts in defense of that infrastructure, and then planning for its protection. That prioritization will be based upon an analysis of risks and vulnerabilities, which will concurrently assist us in developing and implementing protective measures, facilitated by leveraging operational expertise we have already accumulated over the years. In consonance with these efforts, we must develop intelligence capabilities that will correlate threat information, monitor suspicious activity, and issue warnings as appropriate. These intelligence activities will require coordination throughout the governmental sectors—Federal, State, and local—as well as with the private sector. Finally, if the situation should arise, we must be prepared, as a nation, to respond to catastrophic incidents.

The DHS provides leadership to the Nation in driving the implementation of these key activities using a risk management methodology that is driven by a dynamic threat environment. This methodology includes physical, human, and cyber resources in both the public and private sector. It follows a five-step process: identify critical infrastructure; assess vulnerabilities; normalize, analyze, and prioritize; implement protective programs; and measure effectiveness against performance metrics. Throughout the process, we rely on feedback for

correlating threats to mitigation programs and their effectiveness, as well as for continual process improvement. Taken together, this product becomes the National Risk Profile (see figure 1).

This risk management-based methodology drives all of our CIP activities at the sector level and at the National level across the private sector, the public sector, tribal, local, State, and Federal governments.

The first step of the risk management methodology is the identification of critical infrastructure that must be protected. This information is maintained in the National Asset Database (NAD), which we are continuously working with all of our partners to refine. At the Federal level, we aggregate that information into a single database tool, and analyze it to eliminate duplication and to ensure consistency of the level and quality of information from all sources. Using standardized criteria, we also obtain information from the states on their assets across all infrastructure sectors. This information is analyzed to eliminate duplication and to ensure consistency. The database is continually updated to ensure that the data is up-to-date and accurate. Ideally, therefore, we will obtain a national perspective, with the most recent information about key assets from all of the critical infrastructure sectors across the United States.

Within the NAD, we are continuously integrating vulnerability assessment information to correlate vulnerabilities across sites, sectors, and geographies. We gather existing assessment information from

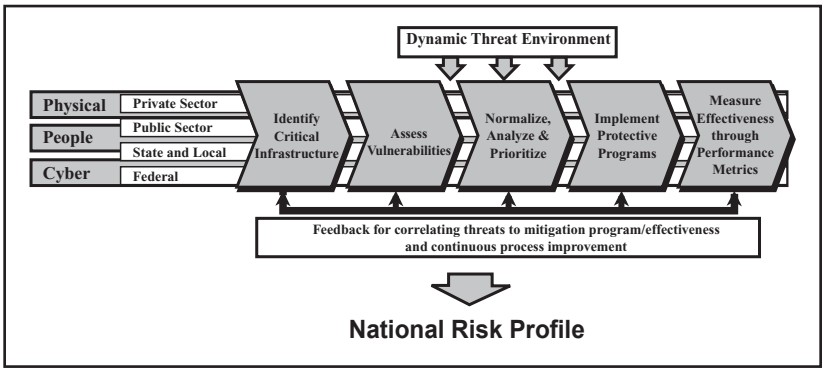

Figure 1: National Risk Profile

government and private sectors and compare asset strengths and weaknesses across sectors and geographies. We conduct vulnerability assessments in the buffer zones surrounding the sites, once again using methodologies from both public and private sectors to determine susceptibility to all types of threats. The results are integrated into the database to produce a single analytical tool for analysis and comparison.

We then use this tool to normalize, analyze, and prioritize protective efforts. Using analytic techniques, we can compare weaknesses and susceptibility to threats across the inventory of known assets to generate relative risk profiles for individual sites, sectors, and segments within sectors. Comparison of the risk profiles across disparate vulnerabilities, sectors, and threats enables us to prioritize protective measures and programs in two threat modes. The first category addresses actions that we should take against an identified threat for which we have intelligence; the second addresses actions that we might take in the absence of specific threat information. Thus, we can continuously modulate the relative priorities of protective measures and programs in alignment with the threat stream.

Using the results of this prioritization either in the presence or absence of specific threat information, the DHS leads the implementation of protective programs through collaboration with all of our key partners. Select and focused protection programs can be coordinated through all levels of government, as well as the private sector, to effectively and efficiently address what will inevitably amount to "local requirements." Our goal is to create "force multipliers" among all of these stakeholders, leveraging the resources of each to drive an efficient, sustainable, effective, and measurable implementation of programs to combat the threat.

Throughout the entire process, we strive to continuously measure our effectiveness at all levels, to optimize our execution and to incorporate lessons learned into every step of our methodology. It is imperative that we continuously improve our procedures and tailor them to our diverse group of customers. To that end, we use numerous criteria to evaluate our effectiveness. Generally, these take the form of a series of questions such as those in figure 2.

Measures of Effectiveness: Optimization through continuous measurement and feedback

- The value of our products to our customers in the public and private sectors (what percentage of our products do our customers use or implement?)
- The speed and efficiency of our channels for information sharing, resource allocation (how long does it take for our partners to send/receive products or information from us?)
- The speed of our implementations (how quickly can our customers implement?)
- The level of interaction during implementation (how often do customers ask for DHS assistance?)
- The sustainability of the implementation (are the implementations foundations that are enhanced over time?)
- The result of the implementation (are vulnerabilities decreased over time?)

Figure 2: Measures of Effectiveness

Several major challenges will still confront the Federal government in executing this risk-management methodology. First, we must remember that CIP is a *national* challenge that cannot be accomplished by the Federal government alone. We must leverage the scale and breadth of State and local resources, and the private sector. Secondly, in most cases, government has no regulatory authority over the private sector to mandate security measures. The government must therefore implement incentives or other non-regulatory means to drive increased private sector engagement. Finally, the government does not own most of the data about critical infrastructure. Most of the data resides within the private sector, reemphasizing once again the critical requirement for cooperation between the public and the private sector.

The private sector faces its own challenges. Traditional risk management and security roles within companies have been segregated in terms of Risk Management Officers (business risk), Chief Security Officers (physical security), and Chief Information Security Officers (cyber security). This segregation of roles presents challenges to effective implementation of the risk management methodology, within a company, and across the Nation. Similarly, enterprise risk management has not traditionally been a board-level governance issue within many private sector companies. Without this level of attention, it is difficult

for operational directors and managers to justify security and risk management investments.

Several recent policy developments, including the mandates contained in Homeland Security Presidential Directive 7 (HSPD-7) and the *Interim National Infrastructure Protection Plan,* will enable the Federal government to address their challenges. However, to successfully execute the national infrastructure protection program locally, we believe that the private sector must take its own lead in risk management. By integrating the roles of operational security from a cyber security and physical security perspective, we believe that the private sector can both increase security and reduce costs. A single enterprise security officer, responsible for all company assets, could increase security through an integrated, holistic approach, and could reduce cost through the elimination of duplicative and non-interoperable tools and processes. Moreover, companies could unify the operational security role with an enterprise risk management function that is responsible for developing and implementing risk management strategies. This approach would provide a complete alignment between the business risk management function and the security operations function. In addition, it could enable business objectives by aligning security operations with business priorities.

Finally, risk management and enterprise security need to be elevated to the board level—good security must be seen as good business. Driving this concept from the top down will ensure that good risk management practices are integrated into every aspect of operations. Such an approach will increase total business resiliency and ability to recover from disruption through the use of consistent risk management and security practices. Costs will be reduced by eliminating duplicative security and risk management investments by line managers.

Such innovation, coupled with the governmental efforts I have described, would align our risk-management-based framework across government and the private sector, resulting in key benefits to the Nation. It would lead to the implementation of a national-wide, systematic, and integrated approach to identifying, prioritizing, and protecting critical infrastructure. It would address a spectrum of concerns spanning physical, people, cyber assets, sector-specific challenges, and the inherent

interdependency of our critical infrastructure and key resources. It would inform decision makers about the implication of threats as they prioritize national, corporate, and public risks. It would provide a common framework for assessing, managing, and mitigating risks across all infrastructures. And finally, it would create a "common language of business" for protection activities across the public and private sectors. In short, these innovations would integrate, through a single framework, our national infrastructure protection program, as Congress envisioned, and as our Nation demands.

Measured Response: Computational Experimentation and Training Environment for Homeland Security[1]

Alok R. Chaturvedi

Purdue Homeland Security Institute

Paul Drnevich

Krannert School of Management

Shailendra Mehta

Krannert School of Management

Introduction

The perceived threat of terrorism in the United States homeland has increased dramatically this decade. Given recent terrorist attacks and evidence of continued threats, governmental agencies at the Federal, State, and local levels face unique and extreme pressures and must make decisions with implications of extreme magnitude. To deal with these unique and challenging new situations government agencies must develop and practice coordinated response strategies for possible terrorist strikes in the United States. The nature of the operational pressure, turbidity, and outcome implications makes this a unique and challenging operating environment. Towards this end, a simulation training exercise series, termed Measured Response, is being conducted by Purdue University to facilitate decision making under these conditions. Through the exercise, Federal, State, and local officials—and others representing the departments of Homeland Security, Health and Human Services, and Transportation—were able to practice response skills and engage in stimulating interaction.

[1] This research is funded in part by grants from National Science Foundation and Indiana State 21st Century Research and Technology Fund

Synthetic Environment for Continuous Experimentation

The Synthetic Environment for Continuous Experimentation (SECE) is developed using the Synthetic Environment for Analysis and Simulations (SEAS) platform [Chaturvedi and Mehta, 1998, 2000, 2002]. SEAS allows the creation of fully functioning synthetic economies, societies, nations, and organizations that mirror the "real world" counterparts in all its key aspects by combining large numbers of artificial agents with smaller numbers of human agents to capture both detail intensive and strategy intensive interactions. Major components of SECE are described below.

The Environment

The environment portrays the background and the contextual structure of the domain for which the synthetic environment is developed. It models the entities and their behaviors, and describes the relationships among them that constitute the simulation's backdrop. The environment contains the geography and the physical details of the space such as the road networks, the structures, traffic patterns and pedestrian dispersion. It also implements the rule sets that guide the interaction of the agents between each other and also with the environment. Hundreds of thousands of software agents, whose emergent behavior defines the environment, are used as a platform with which human players can engage in strategic decision making simulations. The environment in this context is a hybrid of microeconomic analysis combined with models from the fields of operations research and management science, epidemiology, and psychology (although a much different, bottom-up kind of simulation than the typical top-down discrete event simulation). This approach, wherein human players can participate concurrently with an agent-based environment, offers the following benefits:

- The seamless and interchangeable integration of human and software agents. This allows significantly more complex experiments and simulations to be conducted than are usually possible in the fields of experimental Economics (Kagel and Roth, 1995), Psychology (Yantis et. al, 2002), and Epidemiology (e.g. Kaplan, Craft and Wein, 2002). These

experiments can combine depth of decision making (using humans) and breadth (combining artificial agents).

- The consequences of decisions can be measured and analyzed. This extends the purview of traditional decision support from building models that support human decision making to actually being able to gauge the impacts of decisions.
- A laboratory for testing the efficacy of decisions, strategies and tools. Experiments can be devised that measure the effects of various decisions against the support tools used to arrive at those decisions.

The Agents

Situated in the environment are agents. An agent, typically, represents one or more people in a simulation. It can interact with other agents and with the environment. A distinction is made between artificial agents and human agents. The roles of these agents can be interchanged based on the requirements of the problem domain. The behavior of the human players is not pre-determined and they are free to act as they wish under existing conditions that are clearly described and presented to them in an intuitive and informative way. For example, a human agent playing the role of Health and Human Services at the local level may have a certain budgetary allocation, a certain stockpile of supplies, a certain number of hospital beds and a certain authority to screen, isolate, quarantine, and vaccinate. It is up to the person to make decisions in each of these areas.

SEAS's intelligent agents contain autonomous processes that are adaptive and behave like human agents in a narrow domain. In their respective domains, each agent has a well-defined set of responsibilities and authorities so that it can execute its tasks effectively. The agents are programmed to maneuver within their domain from the perspective of micro-macro linkages displayed in their collective behavior model.

In addition to the elemental agent structure, it is necessary to provide a conceptual model for agents to communicate and collaborate in the environment. Since emergent behavior culminates from the nonlinear interactions of agents within the environment and with each other, there must be primitives supplied for facilitation.

Especially critical are the functions of communication and collaboration. The conceptual model for this aspect of agent structure is based upon conceptual ports and channels. A port is a place where an entity submits its outgoing messages to the environment. A port allows its owner to configure its own communication rules. On the other hand, a channel is a place where an owner can query messages from the environment discriminately. Entities that are "interested" in messages will create channels to query the ports for messages. This allows the system to define communication rules prior to runtime. Using the example above, if a human player desires to target children for vaccination, then this would be done by sending a message on his/her port. Also, the children agents would poll messages on this port to see what, if any, messages currently exist of which they should be aware.

Each agent has a set of eight behavior primitives that will enable him or her to perform their actions autonomously. These primitives are Initiate, Search, Evaluate, Decide, Execute, Update, Communicate, and Terminate. Different algorithms are used to differentiate between agents. For example, an agent representing a smart individual will have more sophisticated search and evaluation algorithm than that of a not-so-smart agent.

Live and Computational Experimentation in Smallpox Bio-terrorism

We use an explicit spatial and temporal paradigm to develop agent-based synthetic societies that mimic the essential demographic, epidemiological, and economic characteristics of the United States. The artificial agents are tied to the geography at the city, state and national levels. To make matters tractable, we develop detailed models of a city, a state, and a national command center. Several agencies coordinate their efforts at the local, state and national levels. At least three agencies, the Department of Health and Human Services, the Department of Transportation, and the Department of Homeland Security, are each modeled. Human players play these agencies, singly or in teams. Therefore, we will allow for the interaction of up to fifteen teams of human players. These teams of human players will interact with the decisions of the artificial agents. The human teams will provide the strategic complexity in decision making while the artificial agents will provide the detail. This combination of human and artificial agents will represent a mixture of depth and breadth of decision making simultaneously.

Using this environment we simulate a biological attack on the synthetic population and allow the human teams to respond. Using carefully constructed algorithms that allow the virtual agents to replicate actual human activity, the attack propagates through the virtual population as it would through an actual society. Upon the completion of a scenario, the government officials are informed of the ramifications of their decisions, which they then will be able to analyze for their impact. From this comparison, the officials are able to learn to improve both their decision making and response time. The tool allows officials from each state to test response plans in a risk-free environment, thus enhancing their ability to respond in an actual attack.

The Measured Response (MR) simulation was developed to study questions associated with the deliberate release of biological agents such as smallpox. The main motivation of MR is to increase our understanding of critical factors in spatial, temporal, socio-economic, and political realism.

Multi-layer, Multi-discipline Modeling in SECE

Measured Response is modeled in four layers as shown in figure 1. In the first layer, we modeled the virtual geography that is similar to actual geography. We then created a population of artificial agents where each agent is tied to a different location. The demographics and the distribution of the artificial agents mimic that of the actual population. An overlay of actual infrastructural characteristics models the broad availability of hospitals, roads, railways, and airports. These aspects are crucial in determining the patterns inherent in the spread of infections, as well as the routes by which relief supplies and interventions might arrive. To make matters more tractable, we developed detailed models of a city, a state, and the rest of the United States. We accomplished this by creating over 470,000 artificial agents to represent the total populations of the United States. Approximately, 160,000 agents represent the population of the city (each agent represent 10 individuals – 1:10 granularity); 60,000 agents represent the state (1:100 granularity); and 250,000 represent the rest of the United States (1:1000 granularity).

In the second layer, we model the movement of agents within and across geographies. We develop movement models for normal movements,

morning rush hours, evening rush hours, panic fleeing, and special event related movements. These behaviors are calibrated from the Department of Transportation data and broadly reflect the real situation.

In the third layer, we use an explicit spatial and temporal paradigm to model epidemiology of smallpox at the individual and population levels. We use exposure of susceptible agents (artificial people) to infected carrier agents to model the spread of disease. We model the rate of transmission as a function of population density, mobility, social structure, and life style. The epidemiological characteristics such as susceptibility to infection by age, gender, and race also broadly reflect the real data. The net transmission rates and patterns may be affected by vaccination, treatment, and/or isolation.

Measured Response Scenario

The MR exercise series simulates local, state, and national level consequences of a bio-terrorist attack on a mid-sized city. The objective of the exercise is to develop and analyze policies and operating procedures to manage the public mood, maintain public health, mitigate the risk of contagion, maintain orderly movement of traffic and people, and apprehend perpetrators. The MR exercise enabled participants to work on key response skills, which included risk management, prioritization, communications, incidence management, and cooperation. Key training objectives included practicing the following:

- Resource/risk management under an unconventional crisis situation
- Prioritization, timing, and intensity tradeoffs of response decisions and actions
- Emergent communication strategy development and enhancement
- Real-time incident management and allocation of decision making among different levels
- Execution and effort coordination among different agencies and actors
- Management of public mood and expectations.

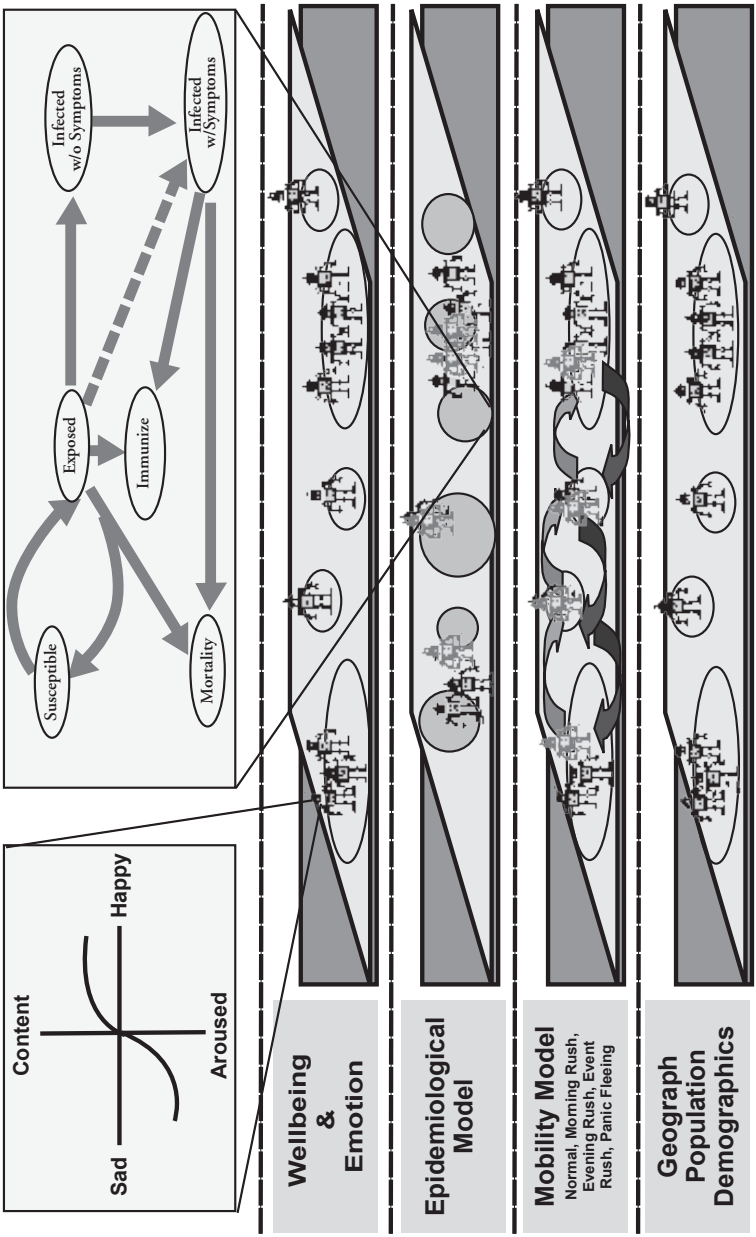

Figure 1: Conceptual Model for Computational Experimentation in Bio-terrorism

Participant Actions

The response to the attack in MR was based on available real-world options and depended on the decisions of the human actors representing their respective government agencies. The decision makers consisted of nine "officials" who were tasked with determining the proper course of action to implement across each of five cities in the state to combat the virus outbreak. The scenario began with local government officials learning that a body (a virtual agent) with an unknown cause of death had been discovered in a downtown hotel in the capitol city. Evidence indicated that the deceased may have been infected with a virus and possibly came in contact while infectious with many people at a downtown music festival. The local government officials faced several choices, each with ramifications that could determine the success or failure of the potential attack. Key response issues included both response timeliness and resources (if and when to involve state and Federal officials) as well as response action and focus (should a quarantined be imposed to isolate the threat, and if so over how widespread of an area?).

Later in the simulation, local officials determined that the initial casualty had indeed initiated a biological attack against the city. State and Federal officials were brought in to assist with mitigating the damages and helping with response and containment. Based on supplied real-world operational data, the government officials were allocated six decision action choices and three commonly accepted levels of intensity to apply to the action. The six response choices were variants of quarantine or vaccination strategies, or no response. The level of intensity varied from neutral/no action, to mild/moderate action, and up to extreme action. The corresponding level of success or failure depended on how the hundreds of thousands of intelligent agents reacted to the governmental actors' responses in the virtual environment.

This set of participant action response strategies can be divided into three main categories consisting of: 1) No Human Intervention; 2) Vaccination; or 3) Quarantine. These strategy choices for dealing with the bio-terror attack on the city, and its potential spread to other cities involve options of quarantine and vaccination response strategies. Vaccination strategies include Mass Vaccination (MV), Trace Vaccination (TV), and City Block Vaccination (CBV). A MV strategy refers to vaccinating 100%

of the population in the all the geographic locations. A TV strategy relies on actual contacts between the infected victims to "trace" the spread of the infection and model a vaccination strategy to "chase" the contagion. A CBV strategy refers to immunizing or treating 100% of the population of a particular geographic location in the hopes of containing or buffering the infection with a "firewall" effect. City blocks are chosen in relation to the outbreak and each of the blocks is vaccinated every alternate day. Quarantine strategies included the more passive City Block Quarantine (CBQ) approach or a more military style, Extreme Quarantine (EQ) approach. The CBQ implies quarantining 100% of the population in a particular geographic location. The EQ implies quarantining 100% of the population in all of the geographic locations.

The intensity of the strategy implementation is correlated with the strategy choice. With a MV strategy a low intensity implementation, in relation to the timing of the response, would vaccinate up to 10% of the population every day until 100% of the population is vaccinated. A high intensity implementation, in relation to the timing of the response, would vaccinate up to 20% of the population every day until 100% of the population is vaccinated. With a TV strategy, a low intensity implementation, in relation to the timing of the response, would vaccinate up to 10% of the population everyday based on the trace model, until 50% of the population is vaccinated. A high intensity implementation, in relation to the timing of the response, would vaccinate up to 20% of the population every day based on the trace model, until 50% of the population is vaccinated. With a CBV strategy, a low intensity implementation, in relation to the timing of the response, would vaccinate up to 10% of the population of the blocks every day, until 100% of the population of the blocks is vaccinated. A high intensity implementation, in relation to the timing of the response, would vaccinate up to 20% of the population of the blocks every day, until 100% of the population of the blocks is vaccinated.

The timing of the vaccination or quarantine strategy implementation assumes no action is taken until the attack is evidenced (days 1 to 4). The response implementation can therefore only take place immediately after the attack (day 5), after slight delay (days 6 to 7), or after extreme delay (day 8). The respective vaccination or quarantine strategy choice is implemented correspondingly. Theoretically and intuitively, earlier

implementations of vaccination or quarantine strategies are expected to have superior results for contagion containment (Kaplan, Craft and Wein, 2002); but prior literature hypothesizes a trade-off in the timing of the response (Chaturvedi, Mehta and Drnevich, 2003). Responding too aggressively, or too early, may adversely impact public mood and produce collateral casualties; responding too late may allow the contagion to grow beyond the control of the responders.

When responding to a terrorist attack, the overall collective goal of the government agencies was to minimize the effectiveness of the attack in terms of contagion spread (infection and death rates) and public perception. While this goal was accomplished to a large extent, it was somewhat complicated by the need to maintain acceptable conditions of public perception regarding the attack. In this, the government agencies must consider the impact on public sentiment that their decisions may have. Specifically, the wider implications of the attack must be considered in terms of the impact and effects on the whole population. For this reason, the public mood (PM) was measured to look at outcomes beyond measures of infection and death rates. The public mood was operationalized as the level of happiness of the artificial agents representing the population and is influenced by the response strategy, intensity, and timing. This construct is based on Maslow's (1968) hierarchy of needs where several factors influence the public mood of the civilian population, simulated by artificial agents, when reacting to a threat in the measured response simulation. These factors include security, basic necessities, health, mobility and freedom, weather, information level, financial capability, and the global economy (Chaturvedi, Mehta and Drnevich, 2003).

Exercise Outcomes, Conclusions, and Lessons Learned

Numerous communication and decision making issues were observed between the departments as well as among the levels of government. Lengthy debates often occurred within departments and between levels of government before action could be agreed upon and then executed. One creative result of this was that "conference call" briefing sessions emerged between rounds where agencies communicated their observations and actions, and coordinated the next steps for the following round. This process appeared to result in a significant improvement in the communications process and likely helped contain the diffusion of the

disease. When MR was concluded, the decision results were studied and compared to preferred optimal outcomes (minimal casualties, contagion containment, and public mood) as well as the results from the prior year's exercise. Communications challenges, response delays, and agency issues were observed in both exercises and appeared to create operational challenges and affect some outcomes. Specifically, these included government officials having a tendency to not communicate early or often enough internally or externally, within and across both levels and agencies. Some participants failed to respond in what was judged to be a timely manner, and others became bogged down in extensive discussions on the type of response action required and the level of intensity of the action chosen. It is hoped that through continued training through this and other similar exercise series, inter-level and inter-agency communications processes can be improved.

These observations indicate that government officials clearly struggled with communications and the decision making process, much as they appear to do in day-to-day, real-life interactions. This mimics real-life experiences, and it may be due in part to a lack of guidelines between and within levels. It is essential that the right people have the right information at the right time. The diagnosis of a bio-terror attack can be done more efficiently when the proper personnel are informed of the events. Despite some of these challenges, the participants in the MR03 exercise were able to successfully coordinate their actions and response choices to contain the outbreak and limit adverse health and economic impacts. Beyond the successful exercise outcome of the MR03 simulation, information on the decision making processes of the participants was captured through a questionnaire. This data provided additional insights, which may prove to be of some value to homeland security practitioners. Items measured included individual objectives and priorities, information usage, and communication needs, as well as confidence, satisfaction, and perceived effectiveness of the response decisions. Findings indicate the following:

- Economic impacts were weighted 30%, health impacts were weighted 70% and these preferences remained fairly constant overall throughout the exercise rounds.
- Initial priorities were high and remained high for Emergency Management, Health Services, Health, Information, Law Enforcement, Mitigation, and Public Mood.

- Initial priorities were moderately high or neutral but declined over the course of the exercise for Energy, Financial, Food Supply, Public Order, Relief, Transportation, and Water Supply.
- Participant perception of the effectiveness of the response-decisions ranged from moderate to very effective and increased throughout the exercise rounds.
- Participant perception of the satisfaction of the response-decisions ranged from moderate to very satisfied and increased throughout the exercise rounds, peaking after the third round, and declining slightly by the end of the exercise.
- Participant perception of the confidence of the response-decisions was moderate to very confident and increased throughout the exercise rounds.
- Participant perception of the information for the response-decisions was moderate, but increased throughout the exercise rounds.
- 20% of Participants viewed the outbreak as contained after the first round, 60% after the second, 40% after the third, and finally 55% thought the outbreak was contained at the end of the exercise.
- Participant perception of the threat level ranged from yellow, to orange, and then towards red as the rounds of the exercise progressed.
- Participants were unlikely to use Mass Quarantine and Mass Vaccination approaches, and these strategies became even less likely as the rounds of the exercise progressed.
- Participants were likely to use City Block Quarantine and Trace Vaccination approaches initially; but these strategies became somewhat less likely, whereas City Block Vaccination become more likely, as the exercise progressed.
- Participants chose a delayed response after some information was available, and this held constant throughout the exercise rounds, though immediate responses were favored in early rounds of the exercise.
- Participants preferred an aggressive response; this held constant through the exercise rounds.

The observations and results of the MR exercise indicate that, with early intervention and effective communication, multi-level responses can be formulated and implemented to successfully contain a bio-terror attack and thereby minimize health and economic impacts on the population. While challenges remain with the communications and response issues, it is hoped that through continued training, using this exercise series, as well as other similar training activities, multil-evel responses can be improved in the future.

References

Chaturvedi, A.R., *Acquiring Implicit Knowledge in a Complex Domain*, Expert Systems with Applications: International Journal, (1993), 6, 23–35.

Chaturvedi, A.R., and Mehta, S.R., *The SEAS Simulation Environment*, Technical Reports, Purdue University, West Lafayette, IN, 519–530. (1998, 2000, 2002).

Chaturvedi, A.R., S.R. Mehta, Daniel Dolk and Richard Ayer (2003). *Creating an Artificial Labor Market Using the SEAS Simulation Environment.* Working Paper. Purdue University.

Chaturvedi, A., Mehta, S., and Drnevich, P. (2003). *Large-scale Mixed Agent Modeling: A Case Study in Bio-terrorism.* Purdue University Homeland Security Institute working paper.

Kagel, John, H. and Alvin Roth (1995). *Handbook of Experimental Economics.* Princeton University Press.

Kaplan, E.H. , D.L. Craft and L.M. Wein, *Emergency response to a smallpox attack: The case for mass vaccination*, Proceedings of the National Academies of Science (PNAS), (July 2002).

Maslow, A.H., (1968) *The Farther Reaches of Human Nature,* Viking Press.

Yantis, Steven, Douglas Medin, Randy Gallistel and John Wixted. *Handbook of Experimental Psychology.* John Wiley and Sons. 3rd ed. (2002).


Prudens
Futuri

The Defense Critical Infrastructure Protection Program: A Mission Assurance Solution

Dan Mathis

Deputy Program Manager and Director of Operations
Defense Program Office for Mission Assurance

Introduction

This paper provides a brief overview of the Department of Defense (DoD) Defense Critical Infrastructure Program (DCIP). The DCIP is an integrated risk management program designed to contribute to DoD mission assurance—the certainty that assigned tasks or duties can be performed in accordance with the intended purpose or plan. Mission assurance requires the identification, assessment, monitoring, and, when necessary, protection of cyber and physical assets critical to the execution of the National Military Strategy (NMS).

The DCIP is responsive to the requirements for DoD identified in HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, dated December 17, 2003.

Program Scope

The DCIP is a comprehensive set of goal-driven activities that includes critical asset and dependency identification and prioritization, assessment of vulnerabilities and risks, and management of risks to physical and cyber assets and associated infrastructures essential to the execution of the NMS. The DCIP is a complementary program linking the mission assurance aspects of Anti-Terrorism/Force Protection (AT/FP), Information Assurance (IA), Continuity of Operations Plan (COOP), and other readiness programs.

Program Approach

The DCIP approach builds on the existing solid program foundation to continue establishment of a defense-wide, comprehensive, fully

integrated, and sustainable program for protecting and assuring defense of designated civilian, national, and international infrastructures critical to the national and economic security of the nation, culminating in a risk-based management solution for decision makers.

Strategy Overview

The Defense infrastructure is a complex, interdependent, and decentralized network of government and private-sector systems, services, people, and processes. The Defense infrastructure includes private sector and other government functions, crosses organizational and political boundaries, and provides goods and services to meet Defense-wide operational and business requirements. It is composed of assets that provide the operational and technical capabilities that are essential to mobilize, deploy, and sustain military operations during both peacetime and war. The Defense Department must ensure that national and international infrastructure dependencies do not adversely affect the military's ability to fulfill its mission of national defense and global force projection.

Defense Critical Infrastructure Program efforts ensure that essential capabilities are available when DoD needs them. In addition, certain critical infrastructures, key resources, national symbols and events, and other potential targets, although not required to support DoD missions, are vital to U.S. national security and vital to the Nation's economic well-being. The DoD will work collaboratively with the Department of Homeland Security (DHS) to ensure the leveraging of DoD capabilities in the assurance and protection of these national critical assets as the President directs.

The Assistant Secretary of Defense for Homeland Defense (ASD[HD]) is the senior DoD official responsible for the planning and execution of DCIP activities and the use of resources to prevent and respond to threats and hazards to critical Defense and designated civilian infrastructures.

The DCIP is concerned with three classes of infrastructure and assets:

- DoD-owned infrastructures and assets that support the NMS.
- Non-DoD infrastructures and assets that support the NMS, such as:
  - Defense Industrial Base (DIB) – The DIB provides Defense-related products and services that are essential to mobilize, deploy, and sustain military operations.
  - Commercial Infrastructure – Commercial infrastructure provides the power, communications, transportation, and other utilities that DoD warfighters and support organizations must rely upon to meet their respective operational needs.
- Non-DoD infrastructures and assets that are so vital to the nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security or economic wellbeing of the nation or could negatively affect national prestige, morale, and confidence.

HSPD-7 states that certain critical infrastructures and key resources, although not required to support DoD missions, are so vital to the Nation that their incapacitation, exploitation, or destruction could have a debilitating effect on the security and economic well-being of this country. The United States Federal departments and agencies will take necessary measures to identify, prioritize, and protect these critical assets.

Responsibility for the identification and protection of these national assets and high-profile events is a joint responsibility, with DHS in the lead. The Defense Department will work collaboratively and partner with DHS to ensure that DoD capabilities are leveraged to support the national security concerns of the United States.

The DCIP's foundation is a capabilities-based, mission-focused framework that provides a comprehensive and integrated risk management process for understanding, ensuring, and, when necessary,

ELEMENTS OF RISK MANAGEMENT STRATEGY	GOALS AND MANAGEMENT INITIATIVES
1. UNDERSTAND RISKS	• IDENTIFY CRITICAL ASSETS AND DEPENDENCIES AND THE IMPACT OF THEIR DEGRADATION OR LOSS • CONDUCT VULNERABILITY AND RISK ASSESSMENTS
2. IMPLEMENT THE PROTECTION PROGRAM	• ACT ON REMEDIATION AND/OR MITIGATION RECOMMENDATIONS
3. RESPOND TO INCIDENTS	• EFFECTIVELY SUPPORT INCIDENT MANAGEMENT
4. PROVIDE ADEQUATE PROGRAM SUPPORT	• ENSURE AN EFFECTIVE CRITICAL INFRASTRUCTURE PROGRAM FOUNDATION
5. ENABLE MANAGEMENT INITIATIVES	• INSTITUTIONALIZE DOD CRITICAL INFRASTRUCTURE POLICY AND THE PROGRAM • PROVIDE AND MANAGE ADEQUATE PROGRAM RESOURCES • FOSTER DEPARTMENT-WIDE COLLABORATION

Figure 1: Elements of Risk Management Strategy

protecting essential defense infrastructures. DoD is institutionalizing this framework within the department through policy; integration into the Planning, Programming, Budgeting, and Execution System (PPBES); and formalization in the DoD acquisition process.

Strategy Elements and Goals

The DCIP Integrated Risk Management Strategy for FY 2006-2011 consists of five major elements (see figure 1). Each element contributes to managing the risks to DoD critical infrastructure and to providing mission assurance or protection of infrastructures and assets critical to DoD missions or national security.

DCIP Global Environment

The Defense Department's national security missions are global. Reductions in the permanent overseas military presence while operating in new, geographically remote locations and the DoD's increasing reliance on outsourcing have resulted in greatly increased dependence on private

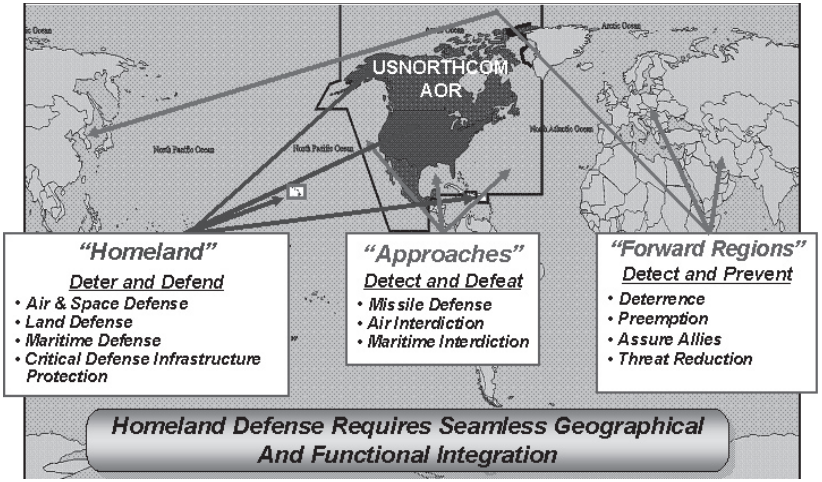

Figure 2: Global Critical Infrastructure Protection

and foreign suppliers of products, services, and infrastructures. The Defesne Department or entities that support U.S. interests neither own nor control most of the infrastructures.

Therefore, DoD must rely on others as it mobilizes, deploys, and sustains military operations. In addition to strengthening partnerships, DoD will institutionalize DCIP requirements for the protection and assurance of foreign and private sector assets and services over time by changing status of forces agreements and the DoD procurement process.

Host nation and transnational infrastructures are the lifelines of our global operating forces. However, the extent of DoD and allied operations' dependence on host nation infrastructures (government and commercial), as well as their vulnerabilities, is not well known or fully understood. Analysis and assessment activities to correct this are underway, but there is still much work to be accomplished in this arena.

CIP Activities

There are six major activities that make up the DCIP: 1) Analysis and Assessment, 2) Remediation, 3) Monitoring and Reporting, 4) Mitigation, 5) Incident Response, and 6) Reconstitution. These activities are illustrated in figure 3.

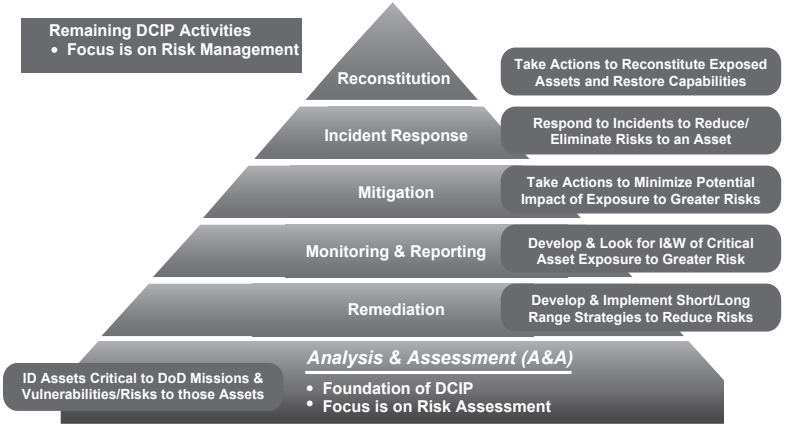

Figure 3: Defense Critical Infrastructure Program Activities

Objectives

The objective of the DCIP is to significantly reduce the vulnerabilities of assets critical to DoD missions using a structured, systems engineering, and risk-based management process. This objective statement describes not only what must be done—***"reduce the vulnerabilities of assets critical to DoD missions"***—but also how it is to be done—***"using a structured, systems/risk based management process."***

Since the DCIP objective is to reduce the vulnerabilities of assets critical to DoD missions, three root questions must be answered:

- Is it critical to DoD missions?
- Is it vulnerable?
- What can be done about it?

These three questions form the basis for the risk assessment that is the foundation of the risk management process.

DCIP Vulnerability and Impact Assessments

The Full Spectrum Integrated Vulnerability Assessments (FSIVAs) is the DCIP standard vulnerability assessment program. It is modular in nature, allowing assessment teams to conduct assessments on one or more modules. The existing FSIVA modules are listed in figure 4.

- Information Security
- Operational Security
- Plans
- Safety
- Personnel/Industrial Security
- Security of Biological Critical Assets
- Security of Chemical Critical Assets
- Security of Nuclear Critical Assets
- Supporting Infrastructure Networks
- Availability of Supporting Material and Services
- Physical Security

Figure 4: FSIVA modules current in 2004

The primary purpose is the identification of vulnerabilities of critical assets. An analysis is conducted on each critical asset to determine the types of damage mechanisms to which the asset is susceptible. These susceptibilities and damage mechanisms may be later matched with known threats that have an ability to leverage that damage mechanism to destroy or render the asset incapable of performing its mission. The impact of asset loss or diminished capability is determined, and potential mitigation or remediation strategies are developed for each vulnerability. Information obtained will be added to the DCIP Data Management System (DMS) by organizations conducting DCIP FSIVAs. This information will be available to combatant commands, services, agencies, and sectors when the loss or degradation of the asset could impact their ability to conduct or support operations. DPO-MA is responsible for coordinating this activity for quality assurance purposes.

DCIP Risk Assessment

The final activity is the determination of risk and its associated costs in terms of mission accomplishment. Risk is calculated using the formula shown in figure 5.

R = I*(V*T)
where
R = RISK
I = IMPACT
V =VULNERABILITIES
T = THREAT/HAZARD

Figure 5: Risk Calculation Formula

The application of threat and/or hazard information against the known asset vulnerabilities and impacts of loss or diminished capabilities provides a current view of risk to assets and, ultimately, to mission accomplishment. As threats or hazards against a particular asset come and go and as the severity of impacts on the delivery of mission-required resources (forces, goods and services) rises and falls, so too will risk rise and fall. The understanding of risk by the mission owner permits remediation decisions that are appropriate and accurate, and when necessary, provides for the prioritized selection of critical assets to protect.

SUMMARY

The Defense Critical Infrastructure Program:

- Is about mission assurance.
- Is about understanding interdependencies.
- Is about effects-based defense.
- Is global—from homeland support facilities to forward theater of operations.
- Separating responsibilities based on geography (domestic versus overseas) fails to recognize inherent interdependencies.
- Must treat critical infrastructures as a "system."
- Is an integrating activity to identify:
  - What is Critical?
  - Are Critical Assets Vulnerable?
  - What Can Be Done to Lower Risk?
  - Must be proactive and dynamic.
  - Must apply risk-based management methodology.
  - Is documenting an established, proven analysis and assessment methodology.
  - Can be leveraged for Homeland Security applications.


Prudens
Futuri


Prudens
Futuri